



DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

SPAWARINST 2280.1B
SPAWAR 08-2C
13 July 1992

SPAWAR INSTRUCTION 2280.1B

From: Commander, Space and Naval Warfare Systems Command

Subj: PROCEDURES FOR DISTRIBUTION AND CONTROL OF COMMUNICATIONS
SECURITY (COMSEC) MATERIAL SYSTEM (CMS) MATERIAL

Ref: (a) CMS 4L
(b) CSP 1A
(c) OPNAVINST 5510.1H

Encl: (1) CMS Responsibility Acknowledgement Form
(2) Designation of Responsible Users
(3) SPAWAR Emergency Action Plan Guidance w/attachments

1. Purpose. To update procedures for the distribution and control of CMS material for those SPAWAR codes and activities using the SPAWAR CMS account.

2. Cancellation. SPAWARINST 2280.1A is cancelled.

3. Background. CMS provides for the security of certain highly sensitive cryptographic materials and related publications. All material distributed through the system requires positive accountability from time of entry into the system until time of destruction. COMSEC materials include, but are not limited to, keying materials, basic equipment and components thereof, repair and modification kits, operating and maintenance manuals (KAMs/SAMs), and controlled cryptographic items procured through the CMS. COMSPAWARSYSCOM has a CMS account, and has designated a CMS custodian for SPAWAR. Reference (a) is the basic CMS publication which contains detailed instructions for issuing, accounting, safeguarding and destroying CMS material.

4. Responsibilities

a. COMSPAWAR and Commanding Officers of Local Holder activities are ultimately responsible for overseeing the proper management and security of the COMSEC materials held within the CMS account. They must formally designate the CMS responsible officer, CMS custodian, and alternate CMS custodians.

b. The CMS responsible officer is tasked with acting on the behalf of COMSPAWAR for the handling of routine CMS matters.

c. The CMS custodian and Local Holder custodian are the principal advisors on matters related to CMS and are responsible for the proper administration of the account. They provide guidance on current policy and procedures and are assigned additional duties in article 310 of reference (a).

d. The alternate CMS and Local Holder custodians are responsible for being ready to assume the duties of CMS and Local Holder custodian if circumstances warrant. Per article 315 of reference (a), they have the same duties as the CMS and Local Holder custodians.

e. Responsible users are to comply with security, control, and accountability procedures as defined in references (a) through (c) and this instruction.

5. Procedures. In compliance with reference (a), the following procedures are issued for codes and activities serviced by the SPAWAR account.

a. Headquarters components and other activities using the SPAWAR CMS account will be designated either as Local Holders or responsible users as defined in articles 335 and 310 of reference (a).

(1) Individuals requiring access to, or custody of, CMS material shall be familiar with this instruction and references (a) through (c). Additionally, directors and supervisors of such personnel shall also be familiar with this instruction and references (a) through (c).

(2) Activities designated as Local Holders must execute a Letter of Authorization/Appointment and make updates to it as required by article 301 of reference (a).

(3) Each individual requiring custody of, or access to, CMS material shall execute enclosure (1), and return it to the SPAWAR CMS custodian or Local Holder custodian. Completed forms shall be retained by the CMS custodian for two years after the individual has been removed from CMS responsibilities. An individual's signature signifies acceptance of responsibility for the proper handling, safeguarding, disposition, accounting, and destruction of the COMSEC material issued.

(4) Directors of headquarters organizations not designated as Local Holders must execute enclosure (2) in order to receive CMS material. Enclosure (1) must be completed and signed by each individual listed in enclosure (2). Persons named in enclosures (1) and (2) must possess a security clearance commensurate with the security classification of the material being handled. Enclosure (2) will be updated upon transfer or reassignment of primary or alternate users and/or directors.

(5) Directors of headquarters components and/or activities designated as either Local Holders or responsible users must develop an emergency action plan. Enclosure (3) contains guidance and is an effective plan which may be used as a

pattern for local emergency action plans. A copy of this plan must be submitted to the SPAWAR CMS custodian for approval. Copies of approved plans must be forwarded to the SPAWAR Security Office by the SPAWAR CMS custodian. Emergency action drills will be conducted on a semiannual basis.

b. Stowage of CMS material must be in accordance with the provisions of references (a) through (c). The combination to each vault, safe, and equipment cabinet holding CMS material which is not subject to two-person integrity (TPI) controls shall be kept on file in the SPAWAR Security Office for access in the event of an emergency. For activities not located in the SPAWAR headquarters building, combinations shall be held by the appropriate local security office as designated by the SPAWAR Security Office. For safes and cabinets afforded TPI, combination envelopes must be sealed in accordance with reference (b), article 205.I and maintained in the SCIF space (room 1132) clearly labeled with the word "INNER" or "OUTER" to designate which combination is contained therein. Combinations must be changed every six months, and upon transfer or removal of an individual having access.

c. Only personnel who have executed enclosures (1) and (2) will be authorized to pick up CMS material. Two persons are required to receive TPI materials. CMS materials shall be checked for accuracy and receipted for using either a CMS 17 card or SF 153. CMS materials shall be transported in a suitable container. CMS material will be issued either on a daily or monthly basis and when directed for an emergency supersession.

(1) Keying materials and Watch-to-Watch Custody Logs issued on a monthly basis shall be picked up from the SPAWAR CMS custodian on the first working day of each month.

(2) Emergency supersession of materials occurring during normal working hours will be handled by the CMS custodian. After normal working hours the Command Duty Officer will immediately notify the CMS custodian. The CMS custodian will determine and initiate the appropriate action.

d. CMS materials not in use shall be placed in a lockable container. Keying materials shall always be under two-person control and stored in a container which ensures TPI. Keytape segments and keycards shall not be removed from the canister or book until immediately prior to the effective period and are needed for use. Individual keytape segments retained for future use during the crypto period will be properly resealed in an envelope until either used or destroyed. Upon suspicion that an item may be missing, the SPAWAR CMS custodian must be notified immediately.

13 July 1992

e. Destruction of keying material shall be in accordance with Chapter 9 of reference (a) and reference (c). Under no circumstances will keying material be destroyed later than 12 hours after supersession except on weekends and holidays where the time limit has been extended to 96 hours (i.e., before noon of the next working day) as specified in reference (c).

f. A current and accurate CMS 25 (Keying Material Destruction Report) and a Watch-to-Watch Custody Log shall be maintained in the working space for sighting by the SPAWAR CMS custodian and alternates.

(1) The monthly Watch-to-Watch Custody Log will list all items retained in that organization's possession. Forms shall be completed by designated responsible users. Any item not physically seen during the watch will have a line drawn through the appropriate block. Items seen shall have an "X" placed in the appropriate block. Materials requiring TPI will be cited and signed by two persons in the Watch-to-Watch Custody Log.

(2) The monthly Watch-to-Watch Custody Log and CMS 25 forms shall be returned to the SPAWAR CMS custodian during the issuing of the next month's CMS materials.

g. The SPAWAR CMS custodian shall be immediately notified:

(1) When there is a suspected loss or compromise of CMS material.

(2) When there is evidence, however slight, of a possible security violation.

(3) When any person having custody of CMS material is absent from work for reasons other than authorized leave, liberty, or travel.

(4) When making requests to obtain, return or relocate any COMSEC materials.

(5) Before any modification or maintenance of CMS equipment is to be performed and upon its completion.

(6) When any CMS material is received through channels other than the SPAWAR CMS custodian.

(7) Anytime a person is in doubt as how to handle a COMSEC related issue.

h. The SPAWAR CMS custodian shall immediately notify the SPAWAR Security Office of any information reported in response to paragraph g(1), (2), or (3) above.

13 July 1992

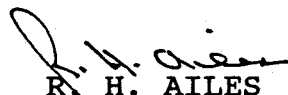
i. In addition to the page-check procedures outlined in article 601 of reference (a), all page-checks of amended publications must be signed by the person making the change and verified (initialed) by a second individual.

j. If residue from an amendment or modification is more than one page, a page-check of the residue must be conducted and notation made that the required residue is present. Amendment residue shall be returned to the CMS custodian for destruction within five days after entering the amendment.

k. Transfer of CMS materials may only be effected through the SPAWAR CMS custodian. No CMS materials shall be removed from the building in which they are located without the knowledge of the CMS custodian (or alternate custodian if the CMS custodian is absent).

l. Each Local Holder custodian shall conduct sight inventory of all CMS material when directed by the SPAWAR CMS custodian. The inventory shall be submitted to the SPAWAR CMS custodian not later than two days after notification that an inventory is required.

6. Action. All personnel involved with or having access to CMS materials shall comply with all the appropriate procedures in references (a) through (c) and this instruction for the handling of CMS material. Random unannounced inspections and drills will be conducted by the CMS custodian and alternates, at the discretion of the CMS responsible officer, to ensure that all COMSEC policies and procedures are adhered to or are in compliance. Non-compliance with these policies and procedures may subject the individual to loss of access to COMSEC materials and disciplinary action.


R. H. AILES

Rear Admiral, U.S. Navy

Distribution:
SPAWAR List 2

Stocked: (25 copies)
Room 113 (SPAWAR Directives and Forms)

JUN 13 1992

ACKNOWLEDGEMENT OF RESPONSIBILITY FOR COMMUNICATIONS SECURITY
MATERIAL SYSTEM (CMS) MATERIAL

NAME

OFFICE CODE

OFFICE PHONE NO.

1. I hereby acknowledge that I have read and understand SPAWARINST 2280.1B.

2. I assume full responsibility for the proper handling, safeguarding, accounting, transfer, and destruction of CMS material held in my custody and/or used by me or those under my supervision. I have knowledge of and will keep myself informed of pertinent articles in SPAWARINST 2280.1B, CMS 4L, OPNAVINST 5510.1, letters of promulgation of publications held, operating instructions on equipment under my cognizance, and U.S. Navy Regulations which set policies, procedures, and responsibilities for the safeguarding of CMS material.

3. I have received instructions on the handling and safeguarding of CMS material. If at any time I am in doubt as to the proper handling of CMS material, I will immediately contact the SPAWAR CMS custodian at 602-1571/4022.

4. Before departure on leave in excess of 45 days and upon detachment from this command, I will check out with the HQ SPAWAR CMS custodian.

Signature

Date

Enclosure (1)

SPAWARINST 2280.1B

JUN 13 1992

From:

To: Commander, Space and Naval Warfare Systems Command
(SPAWAR 08-2C)

Subj: DESIGNATION OF RESPONSIBLE USERS

Ref: (a) SPAWARINST 2280.1B

1. In accordance with reference (a), the personnel listed below are designated as CMS responsible users, and are authorized to receive and courier such material as required.

<u>NAME</u>	<u>RANK/GRADE</u>	<u>SECURITY CLEARANCE</u>	<u>SIGNATURE</u>
<u>Primary Users:</u>			
_____	_____	_____	_____
_____	_____	_____	_____
<u>Alternate Users:</u>			
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Director's Signature

Enclosure (2)

JUN 13 1992

EMERGENCY ACTION PLAN GUIDANCE

1. As required by references (a) and (b), all commands holding classified COMSEC material or equipment are required to maintain a workable Emergency Action Plan (EAP) in order to safeguard the material against compromise and/or exploitation.

2. The EAP is divided into two parts: the first part covers natural emergencies, such as floods, fire, etc. The principle covering this part of the EAP is that of securing as much material and equipment as possible during life and death situations. The second part of the EAP covers operational emergencies, such as riots, civil disorder, or enemy attack. In the event of an operational emergency, it is assumed that the COMSEC material is being sought by the enemy; thus actions should be taken to ensure the destruction of said material. "Partial destruction" is a preliminary step designed to destroy all material not actually in use at the time of the emergency. By conducting a partial destruction, this enables expeditious completion of a full destruction if deemed necessary at a later time. Commands within the contiguous 48 states are not required to have EAP covering operational emergencies.

3. The natural emergency section of the EAP lists procedures to be followed in the event of a natural emergency. The operational emergency section of the EAP would contain two sets of cards, with each card listing a procedure to follow to conduct the emergency destruction. This facilitates the destruction by allowing several procedures to be carried out simultaneously, as well as provide a written copy of what actually is destroyed.

JUN 13 1992

SPAWAR HEADQUARTERS EMERGENCY ACTION PLAN FOR FIRE

1. It is imperative that all personnel be thoroughly familiar with the action outlined in this plan due to the highly sensitive nature of cryptographic and TOP SECRET material.

2. Important factors to consider in case of fire in a space containing classified CMS material are:

a. Safety of personnel.

b. Prevention of damage to cryptographic material while maintaining physical security.

c. Preservation of as much of the classified material as possible.

-d. Removal and subsequent protection of classified CMS material under adequate control and guard.

e. Continual observation of the area until re-entry can be effected.

3. The order to execute this plan shall be issued by the CMS custodian, alternate or higher authority.

4. Attachment B to enclosure (3) gives action procedures and will be prominently posted in the "CMS ROOM" (room 1121, CPK 5).

5. Page 2 of Attachment B to enclosure (3) gives action procedures and will be prominently posted in the "VTC EQUIP ROOM" (room 1103, CPK 5).

6. If classified cryptographic material is destroyed or subjected to possible compromise due to unauthorized viewing or unexplained loss, reports will be submitted by the CMS custodian to higher authority in accordance with reference (a).

7. The procedures herein are meant to complement the procedures of the building's (CPK 5) regular emergency procedures. Thus the building security staff will be tasked to ascertain the seriousness of the disaster (e.g., how long before the fire reaches the affected floor) and also preventative measures (such as manning fire extinguishers). The CMS custodian will be primarily responsible for securing as much equipment as time allows in life or death situations.

Attachment A to
Enclosure (3)

JUN 13 1992

SPAWAR HEADQUARTERS FIRE PREPAREDNESS PLAN

In case of fire, carry out the following instructions, if possible. **DO NOT RISK INJURY!**

FIRE IN CMS ROOM

1. Pull fire alarm located on the wall in passageway next to the stairwell beside room 1131.
2. To secure power, call the building Trouble Desk at 602-1160 (during normal working hours) or call the Duty Officer at 602-8959 (after normal working hours).
3. Remove the fire extinguisher located in the passageway on the opposite wall from the female restroom door and attempt to extinguish the fire.
4. If possible, stow CMS material in safe number 2796 and stow all other classified material in safe number 1594. Remove the CMS Running Inventory from the file binder on the custodian's desk.
5. All non-essential personnel evacuate the area. The CMS custodian will remain in the area until professional fire-fighters arrive, if at all possible, and escort them until all danger has passed.
6. If the vault is damaged to the extent that it cannot be secured after the fire is extinguished, use the Users TPI safe in the VTC equip room (room 1103) until repairs are made.
7. If outside personnel were admitted into the area, conduct an inventory and account for all lost/damaged materials. Obtain the names of all firemen and unauthorized persons for debriefing by the CMS custodian. Submit appropriate reports.

FIRE IN BUILDING, BUT NOT IN CMS ROOM

1. Stow classified CMS material in safe number 2796. All other classified material is to be stowed in safe number 1594. Remove the CMS Running Inventory from the file binder on the CMS custodian's desk.
2. Secure the CMS room door.
3. Evacuate area according to normal procedures.

Attachment B to
Enclosure (3)

JUN 13 1992

FIRE IN VTC EQUIP ROOM

1. Pull fire alarm located in the passageway on the wall opposite to room 1103 door.
2. To secure power, call the building Trouble Desk at 602-1160 (during normal working hours) or the Duty Officer at 602-8959 (after normal working hours).
3. Remove the fire extinguisher located in the passageway on the opposite wall from the female restroom door, and attempt to extinguish the fire.
4. If possible stow CMS material in safe number 0609 and remove safe inventory sheet. Secure the safe and the VTC equip room door.
5. All non-essential personnel evacuate the area. Safety permitting, two of the authorized users will remain in the area until professional firefighters arrive, and escort them until all danger has passed.
6. If the VTC equip room is damaged to the extent that it cannot be secured after the fire is extinguished, use the TPI safe in the CMS room (room 1121) to store any classified or cryptographic material that is exposed, until repairs are made to the VTC equip room.
7. If outside personnel were admitted to the VTC equip room, conduct an inventory and account for all lost/damaged materials. Obtain the names of all firemen and unauthorized personnel for debriefing by the CMS custodian. CMS custodian will submit the appropriate reports.

FIRE IN BUILDING BUT NOT IN VTC EQUIP ROOM

1. Stow classified and CMS material in safe number 0609. Remove safe inventory sheet.
2. Secure safe number 0609, safe number 7570041 and VTC equip room door.
3. Evacuate area according to normal procedures.

Attachment B to
Enclosure (3)